SPYWOLF

Security Audit Report

Completed on
February 8, 2023

SPYWOLF.CO

@SPYWOLFNETWORK

@SPYWOLFNETWORK

OVERVIEW

This audit has been prepared for **OxAI** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✓ Contract's source code
- ✓ Owners' wallets
- ✓ Tokenomics
- ✓ Team transparency and goals
- ✓ Website's age, code, security and UX
- ✓ Whitepaper and roadmap
- ✓ Social media & online presence

> *The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal*
>
> - SPYWOLF Team -

TABLE OF CONTENTS

OxAI

PROJECT DESCRIPTION

According to their website:
"OxAI goal is to enable access to AI computation for anyone in the world, regardless of their resources or location. OxAI will bridge the gap between AI and blockchain to offer powerful AI-based services without compromising data privacy or security."

Release Date: Launched in February 07, 2023
Category: AI

CONTRACT INFO

Token Name
OxAI

Symbol
OXAI

Contract Address
0x428dca9537116148616a5A3E44035Af17238Fe9d

Network
Ethereum

Language
Solidity

Deployment Date
Nov 10, 2022

Verified?
Yes

Total Supply
1,000,000,000,000

Status
Launched

TAXES

Buy Tax
none

Sell Tax
none

Our Contract Review Process

The contract review process pays special attention to the following:

- ✓ Testing the smart contracts against both common and uncommon vulnerabilities
- ✓ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ✓ Ensuring contract logic meets the specifications and intentions of the client.
- ✓ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ✓ Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

CURRENT STATS

(As of February 08, 2023)

Liquidity

1,215,955 USDC

Burn

No burnt tokens

Status:

Launched!

MaxTxAmount

No limit

DEX:

UniSwap

LP Address(es)

0x65717fe021EA67801d1088CC80099004B05B6460

98.9% Locked - Unlocks at 08/03/2023
https://app.unicrypt.network/amm/uni-v2/pair/0x65717fe021ea67801d1088cc80099004b05b6460

TOKEN TRANSFERS STATS

Transfer Count	2882
Uniq Senders	465
Uniq Receivers	903
Total Amount	5307933534785.219 OXAI
Median Transfer Amount	162524437.1312338 OXAI
Average Transfer Amount	1841753481.8824492 OXAI
First transfer date	2023-02-06
Last transfer date	2023-02-08
Days token transferred	3

SMART CONTRACT STATS

Calls Count	9363
External calls	607
Internal calls	8756
Transactions count	3201
Uniq Callers	582
Days contract called	3
Last transaction time	2023-02-08 16:43:59 UTC
Created	2023-02-06 14:58:47 UTC
Create TX	0x5a6bac44112eefae3af83f2d00851199b0333cb913ba0cffb0a22ed9bf3ae75d
Creator	0xf80876b671796a284c22474a9a74c2e698cfc9cb

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

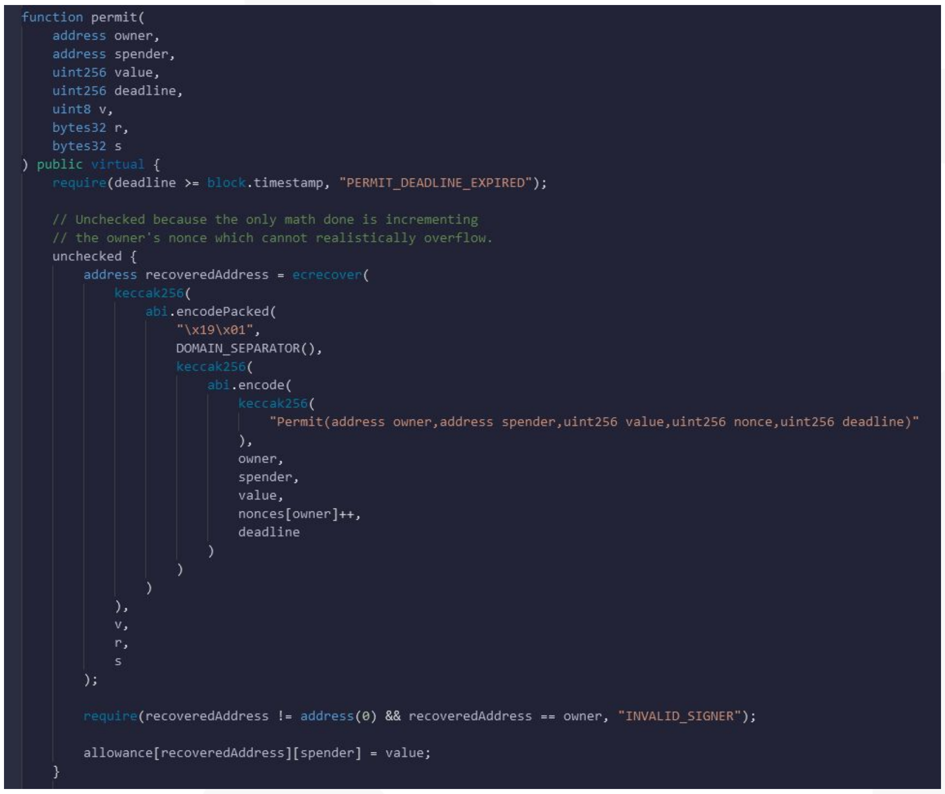
Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠ Low Risk

If any malicious actor manages to obtain signatures from user's account, they will be able to drain contract's native token from their wallets.

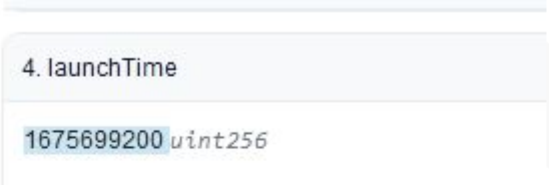


```
function permit(
    address owner,
    address spender,
    uint256 value,
    uint256 deadline,
    uint8 v,
    bytes32 r,
    bytes32 s
) public virtual {
    require(deadline >= block.timestamp, "PERMIT_DEADLINE_EXPIRED");

    // Unchecked because the only math done is incrementing
    // the owner's nonce which cannot realistically overflow.
    unchecked {
        address recoveredAddress = ecrecover(
            keccak256(
                abi.encodePacked(
                    "\x19\x01",
                    DOMAIN_SEPARATOR(),
                    keccak256(
                        abi.encode(
                            keccak256(
                                "Permit(address owner,address spender,uint256 value,uint256 nonce,uint256 deadline)"
                            ),
                            owner,
                            spender,
                            value,
                            nonces[owner]++,
                            deadline
                        )
                    )
                )
            ),
            v,
            r,
            s
        );

        require(recoveredAddress != address(0) && recoveredAddress == owner, "INVALID_SIGNER");

        allowance[recoveredAddress][spender] = value;
    }
```

- Recommendation:
    - Users should watch carefully what they sign with their wallets.

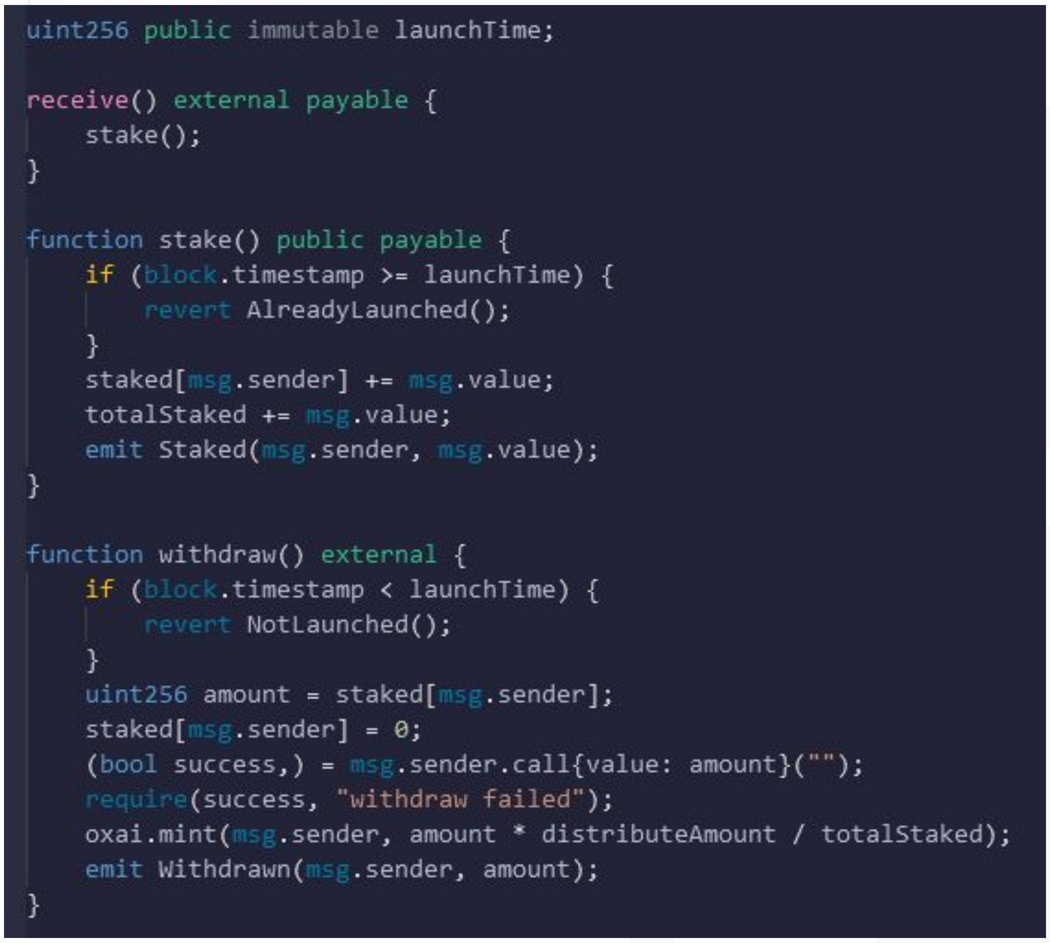
Informational

Project's native tokens were minted via minting contract.
Mint was possible until Monday, February 6, 2023 4:00:00 PM GMT.
launchTime = 1675699200 = Monday, February 6, 2023 4:00:00 PM GMT
Any further call to stake() function or sent ether directly in the contract will revert.
Minter contract can be found at the following address:
0xC4fBCDDb052D8fC51BE901189d5Dd6867197C7d4



4. launchTime

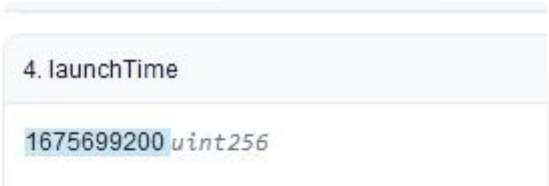
1675699200 *uint256*



```
uint256 public immutable launchTime;

receive() external payable {
    stake();
}

function stake() public payable {
    if (block.timestamp >= launchTime) {
        revert AlreadyLaunched();
    }
    staked[msg.sender] += msg.value;
    totalStaked += msg.value;
    emit Staked(msg.sender, msg.value);
}

function withdraw() external {
    if (block.timestamp < launchTime) {
        revert NotLaunched();
    }
    uint256 amount = staked[msg.sender];
    staked[msg.sender] = 0;
    (bool success,) = msg.sender.call{value: amount}("");
    require(success, "withdraw failed");
    oxai.mint(msg.sender, amount * distributeAmount / totalStaked);
    emit Withdrawn(msg.sender, amount);
}
```

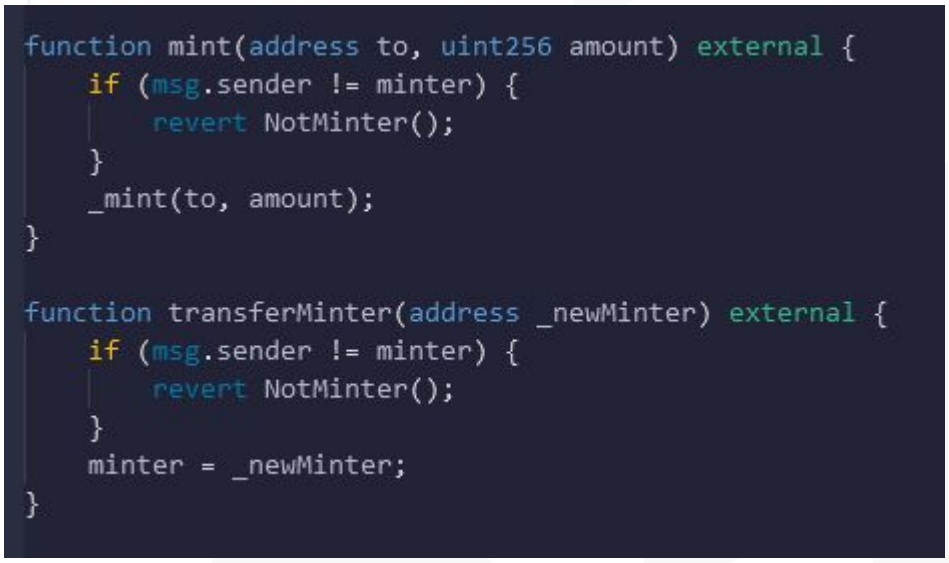
Informational

Minter contract can mint new tokens and transfer the minting role to another address.
The current minter contract do not have transfer minter role functionality and cannot mint new tokens because 'launchTime' is already expired.
launchTime = 1675699200 = Monday, February 6, 2023 4:00:00 PM GMT



4. launchTime

1675699200 uint256



```
function mint(address to, uint256 amount) external {
    if (msg.sender != minter) {
        revert NotMinter();
    }
    _mint(to, amount);
}

function transferMinter(address _newMinter) external {
    if (msg.sender != minter) {
        revert NotMinter();
    }
    minter = _newMinter;
}
```

RECOMMENDATIONS FOR

GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

OxAI

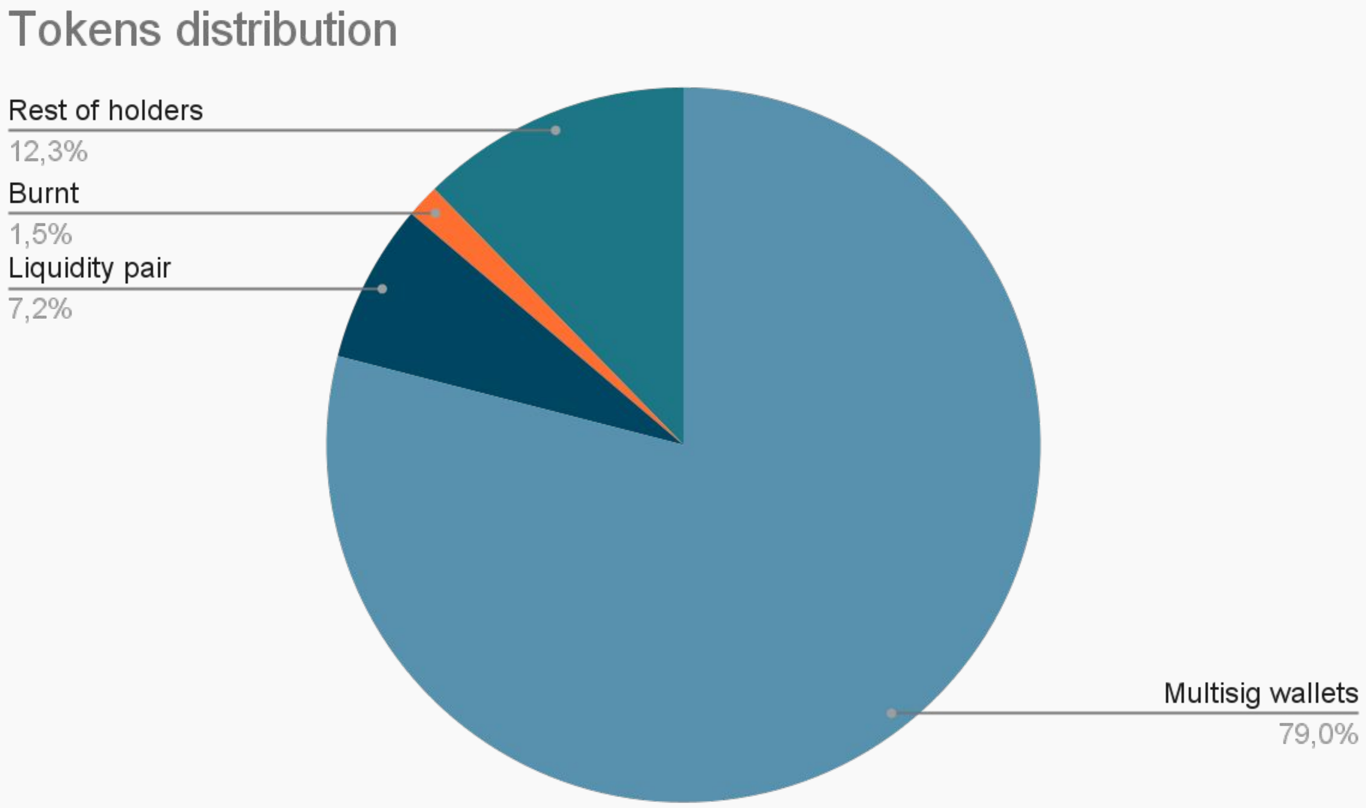
GOOD PRACTICES FOUND

- ✓ The owner cannot mint new tokens after deployment
- ✓ The owner cannot stop or pause the contract
- ✓ The owner cannot set a transaction limit
- ✓ The smart contract utilizes "SafeMath" to prevent overflows

TOKENOMICS

Current distribution according to Etherscan:

- 79% - In 4 multisig wallets
- 7.2% - Liquidity pair
- 1.5% - Burnt
- 12.3% - Rest of holders



Glimpse on the project's initial tokenomics can be found in their whitepaper: https://docs.oxai.com/oxai/tokenomics

THE TEAM

The team has privately doxxed to SPYWOLF by completing the following KYC requirements:

- ID Verification
- Video statement
- Video interview with devs
- Owner's wallet verification

KYC INFORMATION

Issuer

SPYWOLF

Members KYC'd

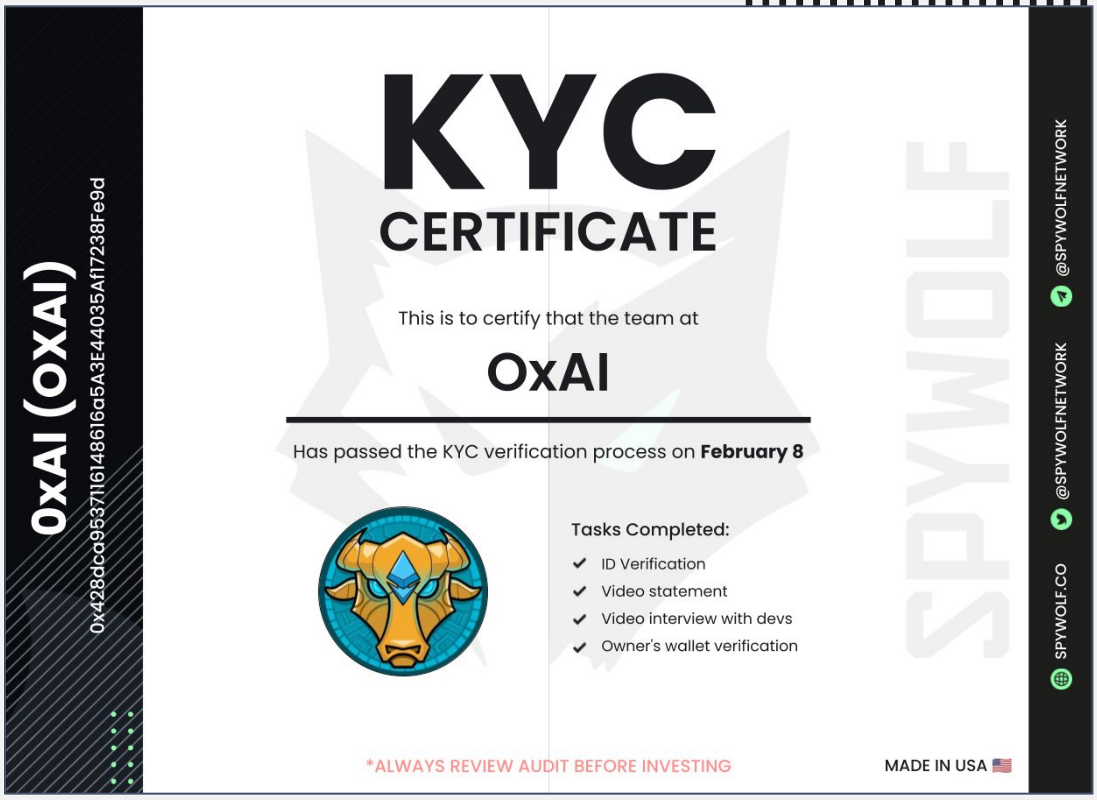
👤

KYC Date

Feb 8, 2023

Format

Image



0xAI (OXAI)

0x428dca9537116148616a5A3E44035Af17238Fe9d

KYC CERTIFICATE

This is to certify that the team at

OxAI

Has passed the KYC verification process on **February 8**

Tasks Completed:

- ✓ ID Verification
- ✓ Video statement
- ✓ Video interview with devs
- ✓ Owner's wallet verification

*ALWAYS REVIEW AUDIT BEFORE INVESTING

MADE IN USA 🇺🇸

SPYWOLF

@SPYWOLFNETWORK

@SPYWOLFNETWORK

SPYWOLF.CO

Certificate Link

https://github.com/SpyWolfNetwork/KYCs/blob/main/KYC__OxAI_0x428dca9537116148616a5A3E44035Af17238Fe9d.png

WEBSITE

Website URL
https://oxai.com/

Domain Registry
https://www.epik.com

Domain Expiration
Expires on 2023-08-06

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

Design
Very nice color scheme, appropriate graphics and overall layout.

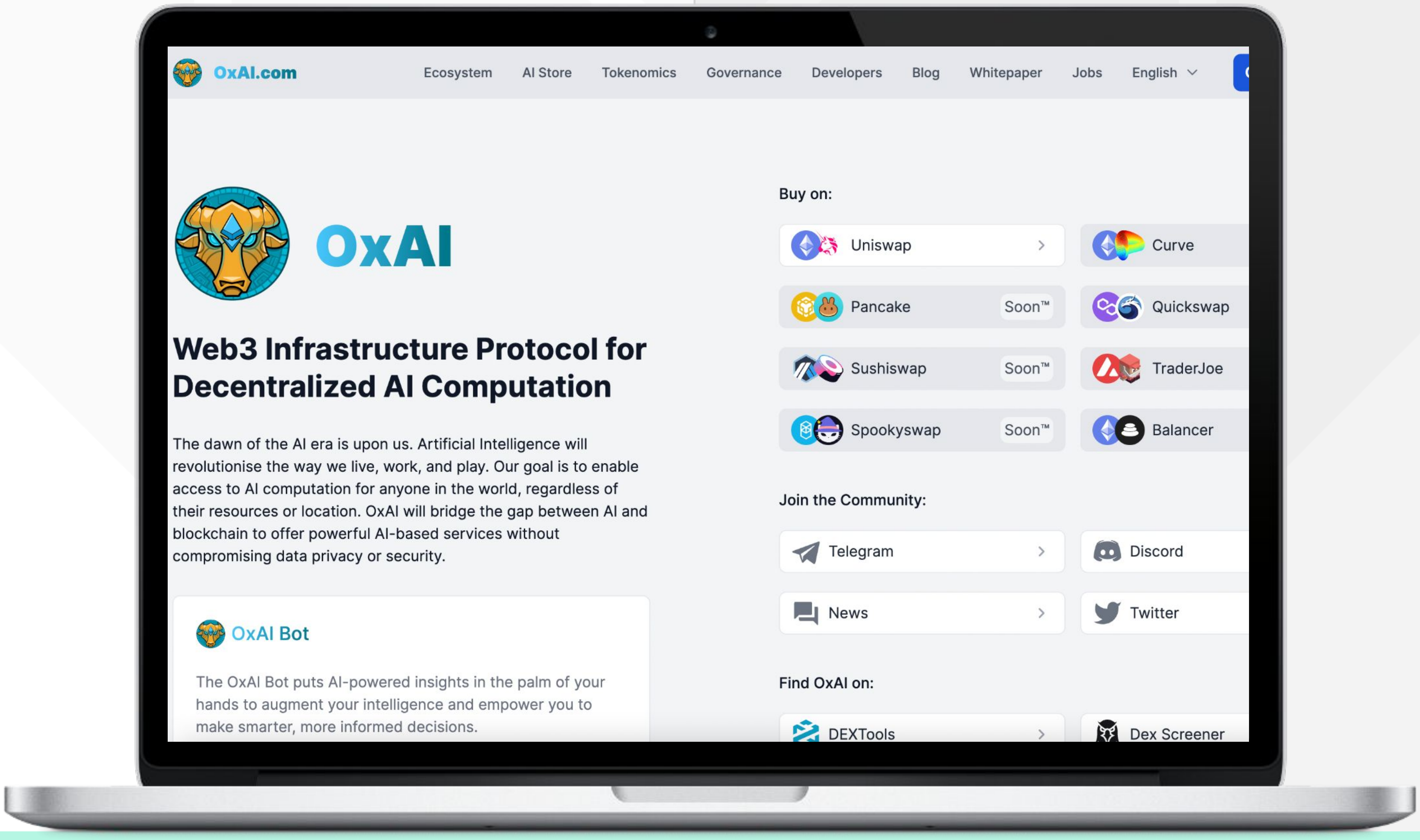
Content
The information helps new investors understand what the product does right away. No grammar mistakes found

.

Whitepaper
Well written, explanatory.

Roadmap
Goals set without time frames.

Mobile-friendly?
Yes



OxAI

Web3 Infrastructure Protocol for Decentralized AI Computation

The dawn of the AI era is upon us. Artificial Intelligence will revolutionise the way we live, work, and play. Our goal is to enable access to AI computation for anyone in the world, regardless of their resources or location. OxAI will bridge the gap between AI and blockchain to offer powerful AI-based services without compromising data privacy or security.

OxAI Bot

The OxAI Bot puts AI-powered insights in the palm of your hands to augment your intelligence and empower you to make smarter, more informed decisions.

Buy on:

Uniswap
Curve
Pancake Soon™
Quickswap
Sushiswap Soon™
TraderJoe
Spookyswap Soon™
Balancer

Join the Community:

Telegram
Discord
News
Twitter

Find OxAI on:

DEXTools
Dex Screener

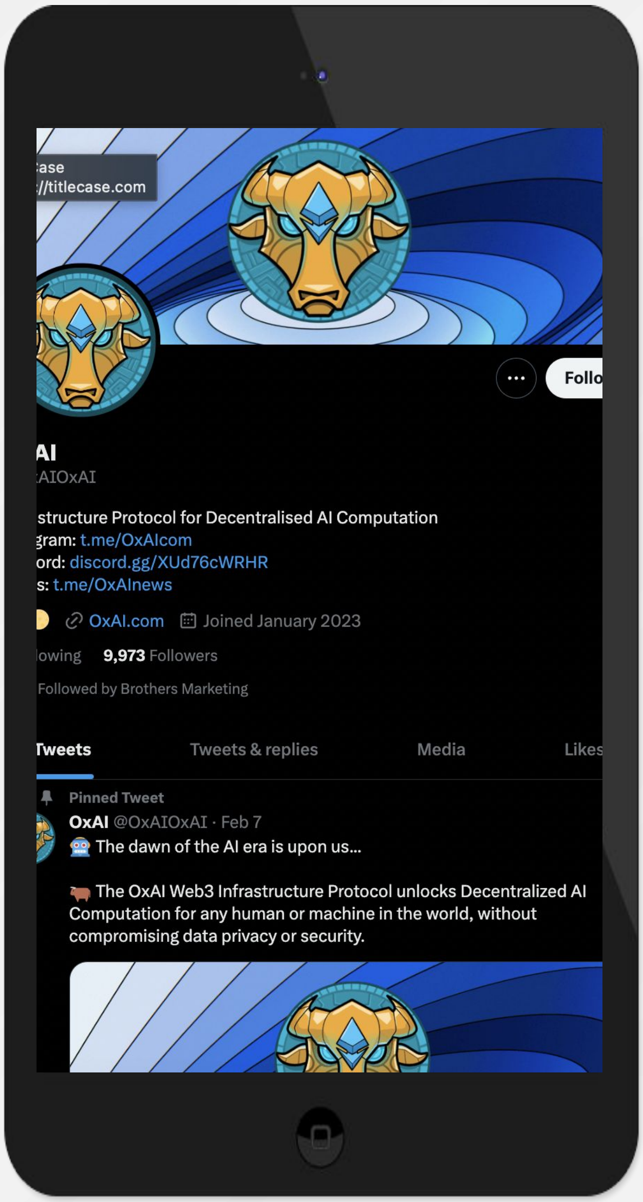
oxai.com

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

Project’s social media community is active and consisted with organic users.



:ase
://titlecase.com

Follo

AI
:AIOxAI

structure Protocol for Decentralised AI Computation
gram: t.me/OxAIcom
ord: discord.gg/XUd76cWRHR
s: t.me/OxAInews

OxAI.com Joined January 2023

lowing **9,973** Followers

Followed by Brothers Marketing

Tweets Tweets & replies Media Likes

Pinned Tweet

OxAI @OxAIOxAI · Feb 7

🤖 The dawn of the AI era is upon us...

🐂 The OxAI Web3 Infrastructure Protocol unlocks Decentralized AI Computation for any human or machine in the world, without compromising data privacy or security.

Twitter

@OxAIOxAI

- 9 971 followers
- Active
- Posts frequently

Discord

https://discord.com/invite/XUd76cWRHR

- 1 836 members
- Active members
- Active mods

Telegram

@OxAIcom

- 8 933 members
- Active members
- Active mods

Medium

- Not available

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- ✓ OVER 400 SUCCESSFUL CLIENTS
- ✓ MORE THAN 500 SCAMS EXPOSED
- ✓ MILLIONS SAVED IN POTENTIAL FRAUD
- ✓ PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS
- ✓ CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.

While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.

No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.

The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.

No applications were reviewed for security. No product code has been reviewed.